

「セキュリティちゃんとしておいて」と言われた方へ

Web診断入門

予算内で進めるための
最適な方法の見極め方

登壇者紹介



株式会社エーアイセキュリティラボ

CX本部プリセールスリーダー **高橋 貴弘**

小売店向けPOSレジサービス等のセールスとして約3年間従事したのち、定期通販向けカートシステム業界にてカスタマーサクセスリーダーを担当。ECサイトにおけるDX推進を100社以上支援し、業務フロー改善やKPI設計にも深く関わる。

2023年より現職。プリセールスリーダーとしてAeyeScanの導入支援に多数携わり、エンタープライズからSaaSスタートアップまで、さまざまな企業の課題解決を支援している。

「セキュリティちゃんとしておいて」と言われても…



何をどこまでやればいいか
わからない

外注まかせで提案が最適か
判断できていない

診断のたびにコストがかさみ
継続が難しい



結果を受け取っても
どこまで修正すべきか迷う

本来の業務に追われ
対応が後回しになっている

正解が見えないまま、手探りで進めざるを得ない状況になっていませんか？

なぜ今、脆弱性診断が「不可欠」とされているのか？

Webアプリケーションに潜む『セキュリティ上の欠陥』を突いた攻撃が、深刻なビジネスリスクとなっています。

重要情報の漏洩

クレジットカード情報や
個人情報、社外秘データの
外部流出

改ざん・データ破壊

Webサイトの書き換えや
データベース内の
重要データの消失・損壊

マルウェアの踏み台

サイト閲覧者への感染、
他社攻撃の「加害拠点」
としての悪用

なりすまし

盗まれた認証情報による
意図しない操作や
決済の実行

DXの加速や開発スピードの向上により、脆弱性の混入リスクはかつてないほど増大

被害に遭えば、サービス停止や信用の失墜、多額の経済的損失は避けられません

診断方法を整理する「2つの軸」

自社に合った方法を見極めるために、まずは代表的な手法の全体像を整理してみます。

Who

誰がやるか

外部委託

プロへ依頼



内製化

自社で実施

How

どうやるか

手動診断

人の目で深くチェック



自動診断

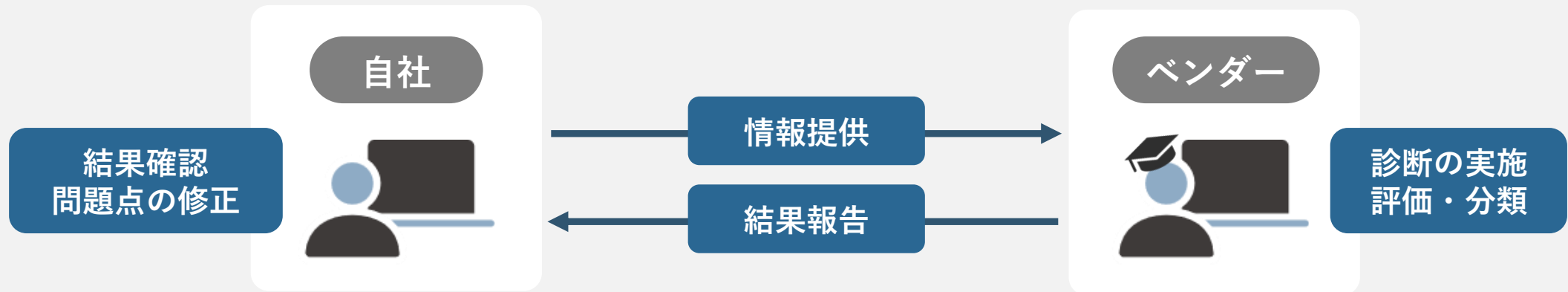
ツールで素早くスキャン

かつての「正解」は、この組み合わせでした

外部委託
プロへ依頼

+

手動診断
人の目で深くチェック



理由

「開発工程そのものが外注」 「第三者診断が必須要件」 「高度な専門性が要求される領域」

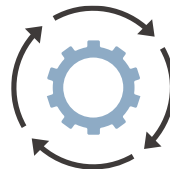
「外部委託100%」モデルは、いま限界を迎えています

セキュリティ人材や 予算の不足



採用・育成は難易度が上昇し
外注先でも同じくリソース不足で
診断できない／リリースできない

アジャイル開発 (開発の高速化)



従来型の診断フロー・期間では
2～4週間のリリースサイクルに
柔軟に対応できない

ローコード開発 (コモディティ化)



PaaS/IaaS/SaaSの普及により
開発のハードルが下がったことで
診断対象サイトが急増している

診断対象・診断回数が増え、外部診断だけでは到底カバーできない

高品質ゆえの「小回りの利かなさ」がボトルネックに

外部委託
プロへ依頼



手動診断
人の目で深くチェック

委託先との連携に
余計な工数がかかる



診断タイミングを
柔軟に調整できない



追加の依頼ができず
リスクを潰しきれない



無理して続けると、調整工数ばかり増えて肝心のリスクが残ってしまう…

IPAからも脆弱性診断内製化ガイドが公開されています

※独立行政法人情報処理推進機構

公開の背景

脆弱性の早期発見が ますます重要に

- ・ 事業継続
- ・ 信頼性維持の観点



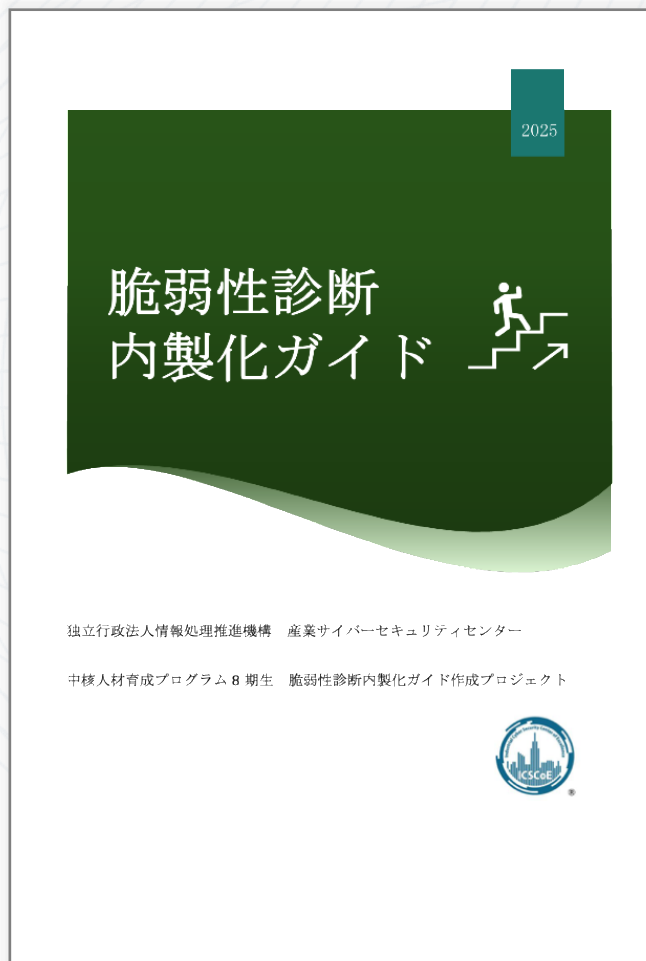
内製化への関心が高まっている

- ・ 新たな脆弱性の増加
- ・ リリースサイクルの高速化



主な内容

- ・ 外部発注と内製の違い
- ・ 内製化に必要な組織体制と人材
- ・ 内製化の進め方と継続的改善プロセス
- ・ 関係組織との連携とセキュリティ意識の醸成
- ・ ツール選定におけるポイント



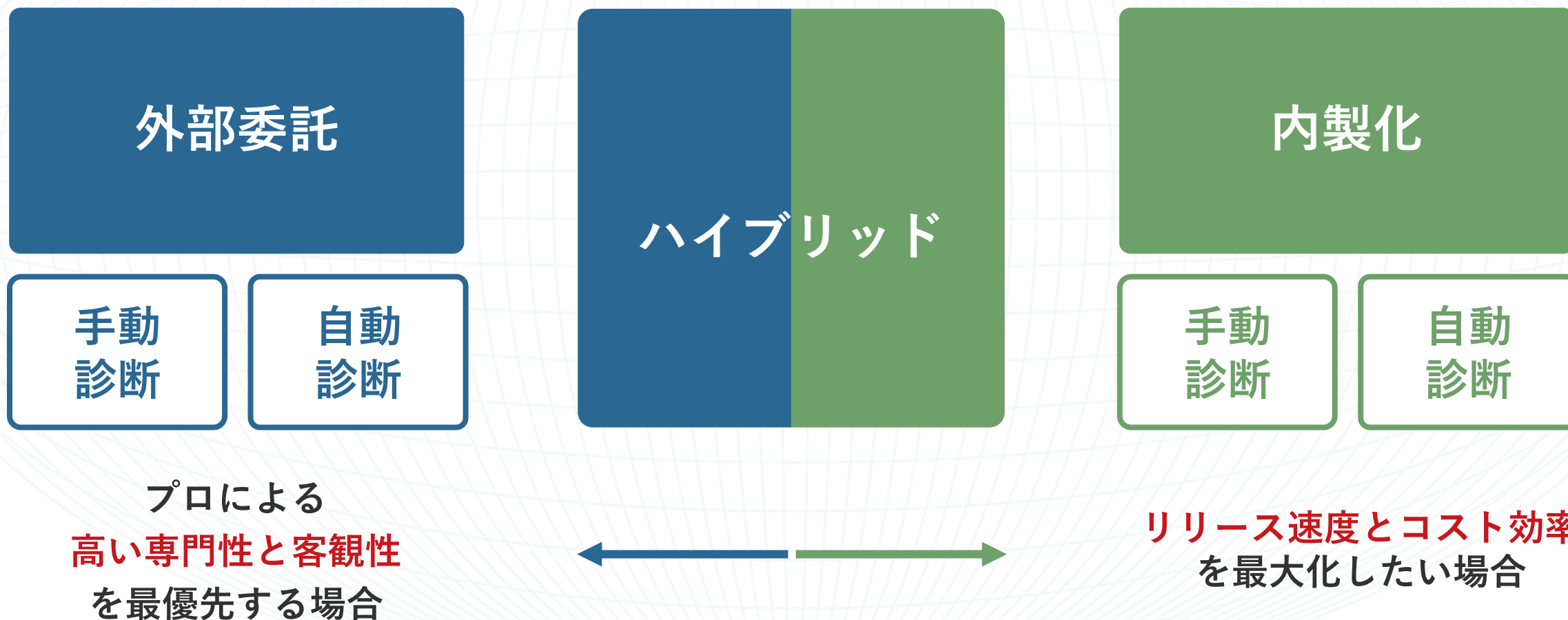
自社に最適な「診断スタイル」を見極めるための比較表

診断方法	特徴	方法	メリット	課題
外部委託	専門業者に依頼	手動診断が多いが 直近では自動診断も登場	専門性が高く高精度 多くの場合「人の目」で チェックが入っている	相対的にコストが高く 各種調整の負担が大きい
ハイブリッド	一部を外部委託するが 残りは自社で診断する	複数手法を組み合わせる	外部の専門性と 内製の機動力を両立	方法の混在によって 管理工数が増加しやすい
内製化（自社実施）	社内セキュリティ部門や 開発チームが診断	脆弱性診断ツールを 利用することが多い	低コストかつ 柔軟な対応が可能 ノウハウも蓄積される	一定レベルの社内人材や 業務フロー/ルールが必要

「外部委託か内製化か」の二択ではなく、
両者の強みを活かす“ハイブリッド型”という選択肢が、いま注目されています

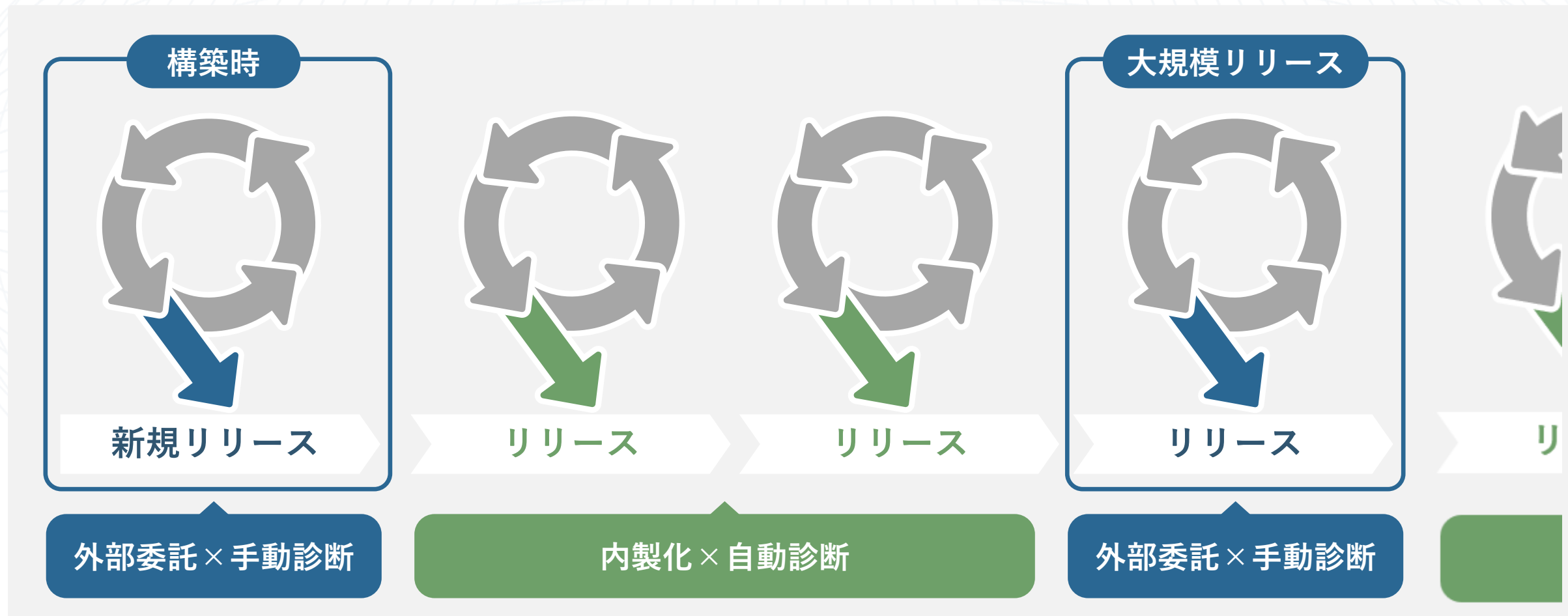
重視する「優先順位」で決まる、3つの選択肢

「品質」「速度」「コスト」のどこに重心を置くかによって、目指すべきスタイルは明確になります。



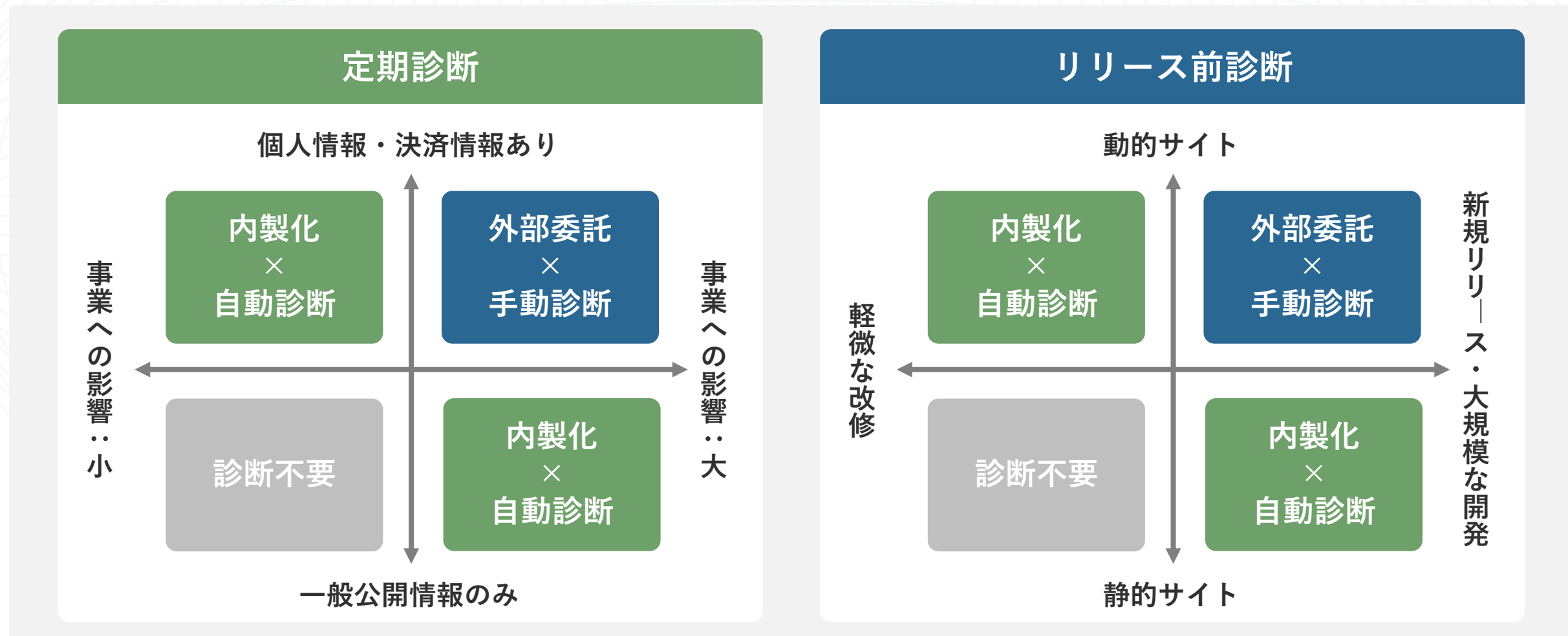
開発サイクルと診断手法の連動イメージ

リリースの規模やタイミングに応じて、外部委託と内製化を使い分ける、実務的な運用モデルをご紹介します。



「定期」と「リリース前」で異なる判断軸

一律にせず、「定期的なリスク確認」と「リリース前の安全検証」で判断の軸を切り分けることがポイントです。



「ハイブリッド診断」を取り入れるための検討項目

守るべき対象の特性と開発現場の実情を掛け合わせることで、無理なく継続できる診断体制が定義されます。

診断対象サイトの重要度

- 取り扱っている情報の重要度
- ビジネス上・業務上の重要度
- 監督官庁・業界団体ガイドライン
- リリース・アップデート頻度



開発内容・体制・タイミング

- 大規模な開発 or 軽微な修正
- 外部ベンダーが開発 or 内製開発
- 部分的に診断 or 全体を診断
- リリース前の診断 or 定期診断

導入事例紹介

カプコン 様



企業名 株式会社カプコン

事業内容 ゲームコンテンツ事業

従業員数 連結 3,531名／単体 3,186名 (2024年3月時点)

課題

共通アカウント管理サービスやゲームのプロモーションサイトなどに対し高頻度な診断ができない状況だった

具体的な課題

- ① 年々サイト数が増えており、外部ベンダーに依頼すると診断するたびにコスト・工数・時間がかかる
- ② 頻度高く診断ができない

共通アカウント管理サービス「CAPCOM ID」を展開するほか、ゲームタイトルごとのプロモーションサイトが年々増え続けており、脆弱性診断のすべてを外注でまかなうにはコスト・工数・時間の観点で課題があった。

導入

技術者でなくても操作できるUI/UXと従量課金ではない料金体系が決め手に

導入の背景

- ① 技術者ではない現場メンバーも使える
- ② 従量課金ではなく同一料金
- ③ 国産ツールのため日本語でサポートしてもらえる

現場主導の診断体制を目指す中で、誰でも使えるUI/UXであることと、FAQやドキュメント、サポートが日本語である点を評価。最適な運用ルールの策定支援など手厚いサポートにより、スムーズに運用を開始。

効果

現場主導の高頻度な診断を実現。
診断工数は1/10と大幅な削減に繋がった

具体的な効果

- ① コスト・時間・工数が大幅に削減
- ② 再診断にかかるコストを気にせず、気軽に実施できる
- ③ セキュリティリスクの低いサイトへの診断頻度も増加

AeyeScanの活用により、セキュアなWebサイト運営とコストや時間、工数の大幅な削減を実現。導入後は、外注時と同等レベルのレポート品質や、実際に巡回・診断したかどうかを画面遷移図で確認できる安心感も評価。

導入事例紹介

NTT東日本 様



企業名 NTT東日本株式会社

事業内容 東日本地域における地域電気通信業務など

従業員数 4,950名 (2023年3月31日時点) NTT東日本グループ 35,500名

課題

アジャイル型・内製の開発体制だが
脆弱性診断は外部に依頼しており
理想とするスピード感でアップデートできない

具体的な課題

- 1 脆弱性診断のみグループ内のセキュリティ専門チームへ依頼しなくてはならない
- 2 希望するスケジュール感で診断できず、ローンチまで時間がかかる
- 3 同じグループ内であっても、サービスの収支という観点でコストが増えてしまう

さまざまなSaaS型サービスを展開する中、より柔軟性のあるアジャイル型の開発を目指し、内製化へシフト。しかし、脆弱性診断は引き続きグループ内のセキュリティ専門チームに依頼する必要があり、スケジュールやコストの面で課題があった。

導入

NTTで作成されている
満たすべき検査項目を
しっかりとチェックできる

導入の背景

- 1 NTTのセキュリティ研究者が作成した絶対条件である検査項目を満たせる
- 2 診断を依頼していたグループ内のセキュリティ専門チームも、すでにAeyeScanを活用していた

さまざまな診断ツールを比較検討していく中で、NTTのセキュリティ研究者が作成した、どのサービスも満たすことが絶対条件となっている検査項目をチェックできないツールもあった。一方、AeyeScanはすべて満たせることから導入を決定。

効果

診断の内製化でアップデート頻度も
大幅に向上。
コスト削減にもつながっている

具体的な効果

- 1 年に1回程度だったメジャーアップデートが複数回できるようになった
- 2 診断回数に関係なく年間利用料だけなので、大幅なコスト削減につながっている
- 3 充実したレポートで、そのまま開発チームに渡してセキュリティ対策が行える

画面遷移図により視覚的に状況がわかることから、メンバーのセキュリティへの理解も深まっている。グループ全体でセキュリティ強化に取り組めるツールだと実感し、今後はAeyeScanを用いた成功事例を社内に横展開していく予定。

とはいえ、診断の内製化ってどうやるの・・・？

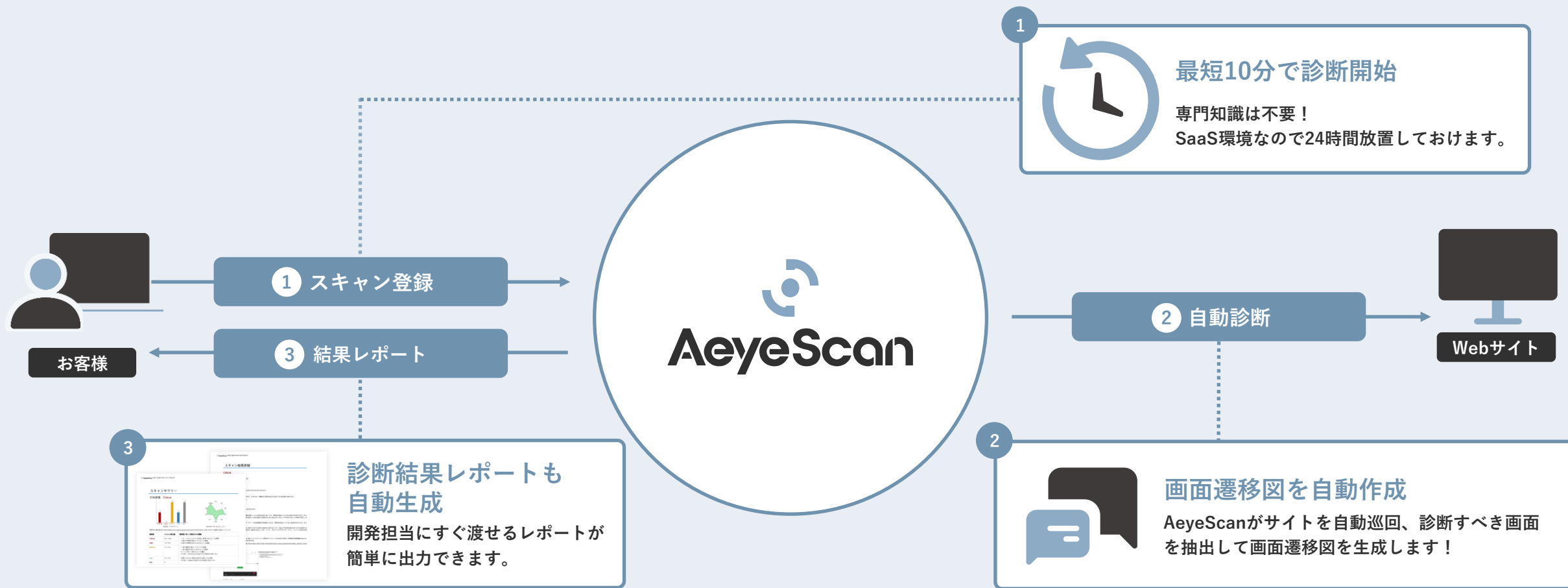
具体的に、診断内製化に踏み出そうとしたとき、課題になりやすいのは「人材」「知識不足」「管理工数」です。

診断方法	特徴	方法	メリット	課題
外部委託	専門業者に依頼	手動診断が多いが 直近では自動診断も登場	専門性が高く高精度 多くの場合「人の目」で チェックが入っている	相対的にコストが高く 各種調整の負担が大きい
ハイブリッド	一部を外部委託するが 残りは自社で診断する	複数手法を組み合わせる	外部の専門性と 内製の機動力を両立	方法の混在によって 管理工数が増加しやすい
内製化（自社実施）	社内セキュリティ部門や 開発チームが診断	脆弱性診断ツールを 利用することが多い	低コストかつ 柔軟な対応が可能 ノウハウも蓄積される	一定レベルの社内人材や 業務フロー/ルールが必要

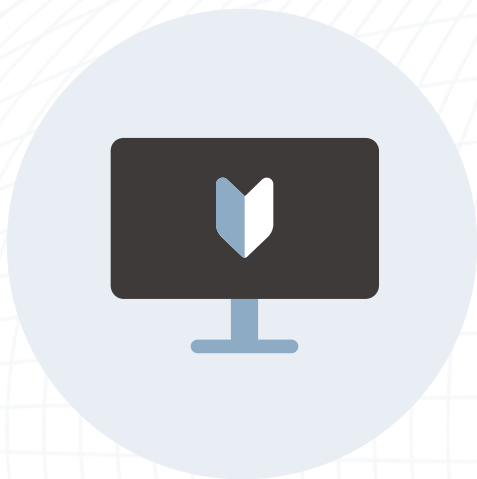
それを解決するのが **AeyeScan** です！

| AeyeScanとは？

AI・RPA活用により、脆弱性診断を自動化するクラウド型Webアプリケーション診断ツールです。



| AeyeScanが選ばれている理由



誰でもかんたん操作



開発やセキュリティの知識がなくても、
トレーニングなしで診断可能。



AIによる自動診断



圧倒的な巡回精度で
24時間自動で診断。
画面遷移図で状況を可視化。



わかりやすいレポート



各種ガイドラインに準拠した
プロ仕様のレポート出力、
日本語と英語に対応。

【簡単＆自動】サイト巡回 → 画面遷移図 → 診断＆レポート作成

画面遷移図

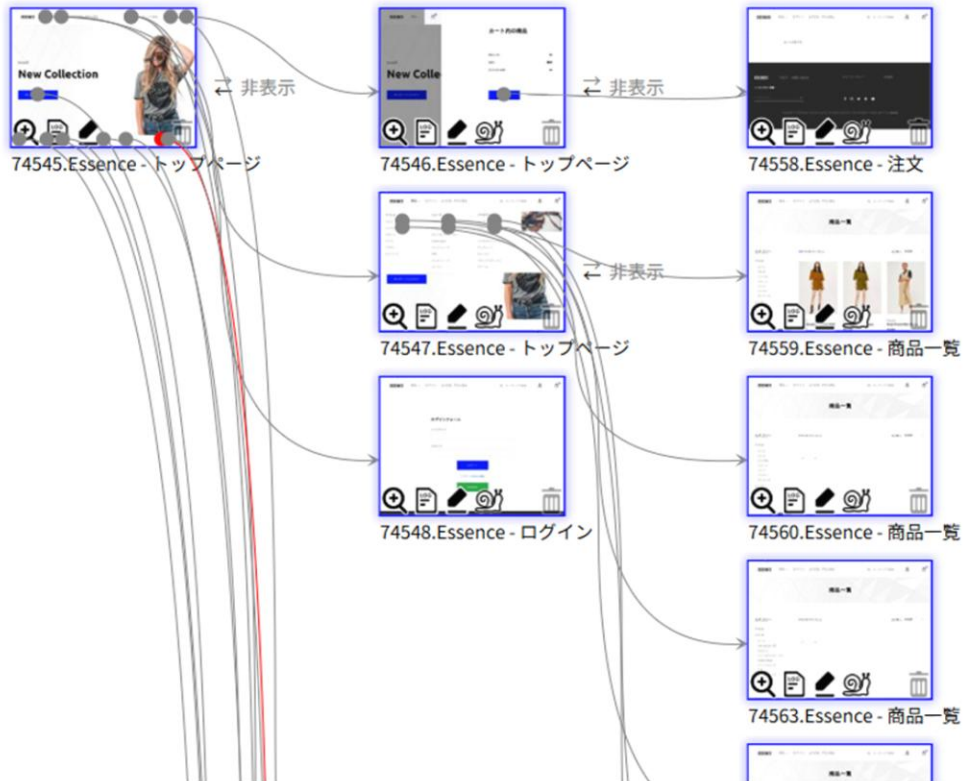
画面数: 86 (スキャン対象: 86)

ダウンロード

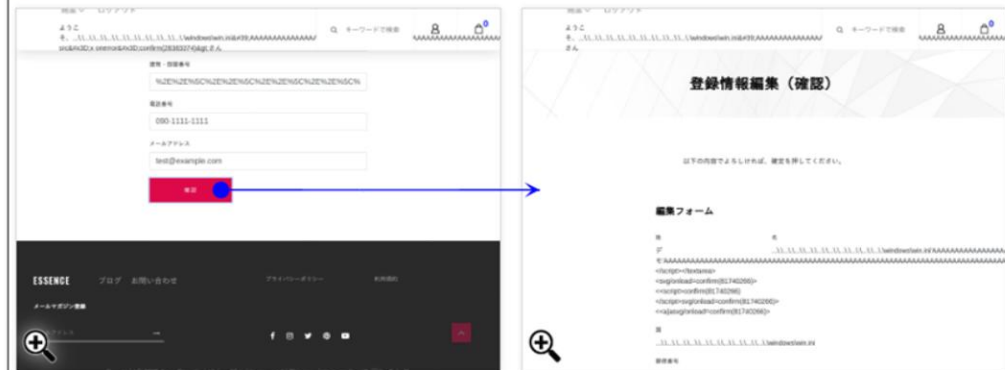
全てを展開

凡例: ⓘ

■ 自動巡回



スクリーンショット



パラメータ情報

タイプ: POSTパラメータ

パラメータ名: last_name

正常パラメータ値: %E3%83%87%E3%83%A2

検知時パラメータ値: %E3%83%87%E3%83%A2"></script></textarea><svg/onload=confirm(81740266)><<script>confirm(81740266)</script>svg/onload=confirm(81740266)><<a|svg/onload=confirm(81740266)>

検知理由

パラメータの送信後に他のページ「Essence - 登録情報編集 (<http://demosite2.aeyescan.work:3333/my-page/user-edit>)」にアクセスしたところ、「81740266」を含んだダイアログが表示されました。

| AeyeScanが選ばれている理由

プロが認める機能・性能

×

誰でも使える操作性

さまざまな企業さまに導入いただいております

ユーザー企業

インフラ※



エンタメ



メディア



製造



金融



人材・教育



SaaS



SI・IT企業



セキュリティ企業



※公共および社会・生活基盤までを包含

社名五十音順（導入いただいた企業様の一部です）会社名及びロゴは各社の商標または登録商標です

| AeyeScanなら！



ガイドライン準拠で
「何をどこまで」が明確に

専門知識不要で
迷わず「内製化」スタート

限られた予算内で
納得感のある継続が可能に



結果から「直すべき優先度」
が分かり、迷わない

自動化で工数を削り、
本来の業務に集中できる

根拠があるから、もう迷わない。セキュリティを、チームの「自信」に変えていく

／最終週もぜひご参加ください／

詳細はこちらから



**8月
限定**

脆弱性対策 まるわかり月間

最終週! Week4 この機会に、診断ツールを見てみませんか?

診断ツールを知る

8月24日(月)～8月28日(金)

セキュリティ診断のお悩み・お困りごとをお聞かせください！

操作性の確認、実際に利用してみたい方へ

AeyeScan の 無料トライアル

トライアルにかかる費用は不要。実際の操作性はどうか？
またどのように脆弱性が発見されるのか？
などの疑問は無料トライアルで解消しましょう。

無料トライアルの申し込み



お見積りの希望・導入をご検討している方へ

AeyeScan への お問い合わせ

お見積りの希望・導入をご検討してくださっている方は
お問い合わせフォームよりご連絡ください。
当日もしくは遅くとも翌営業日にはご連絡を差し上げます。

お問い合わせフォーム





AeyeScan

セキュリティに、確かな答えを。